Europ. J. Combinatorics (1998) **19**, 221–225

On the Relative Davenport Constant

MARIUSZ SKAŁBA†

The relative Davenport constant of products of two cyclic groups with respect to any element is computed. Moreover a new interpretation is proposed and applied to produce quadratic polynomials attaining 'many' successive values with a 'small' number of prime factors.

1. INTRODUCTION

Let us consider a finite abelian group A and a sequence $a_1, \ldots, a_k$ of its elements. It will be called *irreducible* provided no sum of less than k of its distinct elements vanishes.

If in addition $a_1 + \cdots + a_k \neq 0$, then this sequence will be called *primitive*. The *relative Davenport constant $D_a(A)$, of A with respect to $a \in A$* is the greatest integer k with the property that a can be written as the sum of k elements of A forming an irreducible sequence.

For $a = 0$ we obtain the classical Davenport constant $D(A)$, which has been extensively investigated in the literature. The first motivation for considering $D(A)$ was given by Davenport, who observed that this is the maximal number of prime ideals which can appear in the factorization of an irreducible number in a number field, which class group is A. The motivation for the relative version was provided in [6] and relates the number $D_a(A)$ to the maximal number of primes which can appear in the prime decomposition of a natural number, uniquely representable by a binary quadratic form. Recently Davenport's constant was applied in [1] in order to prove that there are infinitely many Carmichael numbers.

Davenport's constant was only computed for very special types of group, for p-groups, for cyclic groups, and for the direct product of two cyclic groups. (See [5]. The case of the product of two cyclic groups is also due to Krujswik, as Mann [2] pointed out.) Certain estimations are also known for all groups (e.g. [1, 3]). The relative version was computed in [6] for the first two types of group and in [7] for the groups $\mathbb{Z}_n \times \mathbb{Z}_n$ (for all its elements). In the present paper we compute it for all direct products of two cyclic groups. The result of our theorem indicates that one cannot expect, in general, a simple expression for $D_a(A)$, relating it only to $D(A)$ and, for example, the order of a (compare [7]).

In addition we want to stress an important link between the classical and relative Davenport constants. Let us fix a non-trivial element $a \in A$ and ask for the greatest number k such that there exists an irreducible sequence $a_1, \ldots, a_k$ with $a_1 = a$. It is easy to observe that $k = D_a(A) + 1$. Therefore the computation of the relative Davenport constants for a given group can be viewed as the first step in the investigation of the structure of 'long' irreducible sequences in A. In the second part of the paper we give an application of this point of view to produce quadratic polynomials attaining 'many' consecutive values with a 'small' number of prime factors—it resembles Euler's polynomial $x^2 + x + 41$ and is based on the classical paper [4].

2. COMPUTATION OF THE RELATIVE DAVENPORT CONSTANT OF THE PRODUCT OF TWO CYCLIC GROUPS

It will be useful to call two elements $a, b \in A$ *conjugate* if there exists an automorphism of A such that $\phi(a) = b$. In such a case we obviously have $D_a(A) = D_b(A)$.

†This work was supported by the Austrian Science Foundation, grant No. M 0038–PHY.

0195-6698/98/020221 + 05 $25.00/0 ej970172

From now let $A = \mathbb{Z}_m \times \mathbb{Z}_n$ be the direct product of cyclic groups $\mathbb{Z}_m$ and $\mathbb{Z}_n$ of orders m and n, where $m|n$. For any integers s, t let (s, t) be the abbreviated form for $(s \bmod m, t \bmod n) \in A$. As in the proof of [6, Theorem 2] we can see that any element of A is conjugate to one of the form (x, y), where $x, y \in \mathbb{N}$ satisfy $x|m$ and $y|n$. Therefore we restrict ourselves in the formulation to such elements.

THEOREM 1. *Let $a = (x, y) \in A = \mathbb{Z}_m \times \mathbb{Z}_n$ where $x|m$, $y|n$ and $d = \gcd(x, y)$. If $d \neq m$ then*

$$D_a(A) = m + n - d - 1.$$

If $d = m$ then

$$D_a(A) = m + n - y - 1.$$

It should be noted that our proof is very close to that of Olson [5]. We need some lemmas.

LEMMA 1 ([5]). *Let E be the elementary abelian group of order p^2 (p prime). If $g_1, g_2, \ldots, g_s \in E$ and $s \geq 3p - 2$, then there exist indices $1 \leq i_1 < \cdots < i_t \leq s$ with $1 \leq t \leq p$ such that $g_{i_1} g_{i_2} \cdots g_{i_t} = 1$.*

LEMMA 2. *If $d = 1$ then the element $a = (x, y)$ is conjugate to an element of the form $(1, z)$.*

PROOF. We will find a unimodular matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that $ax + by = 1$ and $\frac{n}{m}|c$. The last condition ensures that this matrix induces an automorphism of A. Since $\gcd(x, y) = 1$ the general solution of

$$xa + yb = 1$$

is given by the following formulas

$$a = a_0 + ty$$

$$b = b_0 - tx$$

where a_0, b_0 is an arbitrarily chosen specific solution. By an appropriate choice of $t \in \mathbb{Z}$ we can reach $\gcd(a, \frac{n}{m}) = 1$. From now a, b are fixed and we look for $c, d \in \mathbb{Z}$ satisfying $ad - bc = 1$ and $\frac{n}{m}|c$. Again $c = c_0 + ta$ and the desired divisibility can be guaranteed since $\gcd(a, \frac{n}{m}) = 1$. □

LEMMA 3. *If $m > 1$ then*

$$D_{(1,z)}(A) = m + n - 2.$$

If $m = 1$ and $z|n$ then

$$D_{(1,z)}(A) = n - z.$$

PROOF. The equality

$$(m - 1) \cdot (1, z) + (n - 1) \cdot (0, 1) + (s, t) = (0, 0)$$

with appropriately chosen s, t and the fact that the above sequence with $(m-1)+(n-1)+1 = m + n - 1$ elements is irreducible gives the estimation

$$D_{(1,z)}(A) \geq m + n - 2$$

The inequality in the opposite direction results from Corollary 1.1 of [5].

The second part of the lemma follows from Theorem 2 in [6]. □

PROOF (OF THEOREM 1). We proceed by induction on d. For $d = 1$ it is true by Lemma 3. Now let us assume that $d > 1$ and fix a prime p dividing d. Let M_1 be a subgroup of $\mathbb{Z}_m$, N_1 a subgroup of $\mathbb{Z}_n$, with indices $[\mathbb{Z}_m : M_1] = [\mathbb{Z}_n : N_1] = p$. So M_1, N_1 are cyclic groups of orders $m_1 = \frac{m}{p}$,$n_1 = \frac{n}{p}$ respectively. The theorem is true for $Q := M_1 \times N_1$ and $a = (x, y)$ (observe that $a \in Q$) because now $d_1 = \frac{d}{p} < d$. We will prove that any sequence in A of the form

$$a_1 = a, a_2, \ldots, a_{m+n-f}$$

cannot be primitive, where $f = d$ for $d \neq m$ and $f = y$ for $d = m$. Now we write

$$m + n - f = p(m_1 + n_1 - f_1) = 1 + (m_1 + n_1 - f_1 - 2) + (2p - 1)$$

and using Lemma 1 we argue in the the same way as in the proof of Theorem 1 in [5] (the summand 1 counts the element a). This induction step is possible because in both cases $m_1 + n_1 - f_1 - 2 \geq 0$. So we have proved

$$D_a(A) \leq m + n - f - 1.$$

The opposite inequality follows in the case $d \neq m$ from the following equation

$$a + (m - 1 - d) \cdot (1, z) + (n - 1) \cdot (0, 1) + (s, t) = (0, 0)$$

where $a = d(1, z)$ by Lemma 2. In the second case we consider

$$a + (n - 1 - y) \cdot (0, 1) + (m - 1) \cdot (1, 0) + (1, 1) = (0, 0)$$

where $a = (0, y)$. This finishes the proof of the theorem. □

3. APPLICATION TO THE NUMBERS IN MÖLLER'S REGION

The following considerations are based mainly on the paper by Möller [4] and, in particular cases, improve its results.

Let $F = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary field, where d is a square-free natural number and D is its discriminant. Moreover let $\alpha = 0$ if $d \equiv 1, 2 \bmod 4$ and $\alpha = 1$ if $d \equiv 3 \bmod 4$. The numbers 1 and $\omega = \frac{1}{2}(\alpha + \sqrt{D})$ constitute a $\mathbb{Z}$-basis of the ring $\mathcal{O}_F$ of algebraic integers of F. We will call the following subset of $\mathbb{Z}^2$

$$\mathcal{G}(d) = \left\{(x, y) \in \mathbb{Z}^2 : 0 < y \leq \sqrt{-D}, -\frac{\alpha}{2}y \leq x < \delta - \frac{1}{4}(y + \alpha)^2, \gcd(x, y) = 1\right\},$$

the *Möller region of* F, where $\delta = N(\omega)$. The following theorem is due to Möller [4].

THEOREM 2 ([4]). *If* $(x, y) \in \mathcal{G}(d)$ *then* $x + y\omega \in \mathcal{O}_F$ *is irreducible.*

As a corollary one obtains

COROLLARY 1 ([4]). *If* $(x, y) \in \mathcal{G}(d)$ *then*

$$\Omega(N(x + y\omega)) \leq D(Cl(\mathcal{O}_F))$$

where $\Omega(m)$ *denotes the number of primes dividing* m*, counted with multiplicities and* $Cl(\mathcal{O}_F)$ *is the class-group of* F*.*

If one assumes, in addition, that the number $x + y\omega$ belongs to a certain prime ideal $\boldsymbol{p}$, then the above estimation can sometimes be improved.

COROLLARY 2. *If* $(x, y) \in \mathcal{G}(d)$ *and* $x + y\omega \in \boldsymbol{p}$, *where* $\boldsymbol{p}$ *is a non-principal prime ideal then*

$$\Omega(N(x + y\omega)) \leq D_{[\boldsymbol{p}]}(Cl(\mathcal{O}_F)) + 1$$

where $[\boldsymbol{p}]$ *denotes the class of* $\boldsymbol{p}$ *in* $Cl(\mathcal{O}_f)$.

PROOF. It follows from the remark given at the beginning of the paper. □

EXAMPLE 1. Let $F = \mathbb{Q}(\sqrt{-862})$. Then $Cl(\mathcal{O}_F) \cong \mathbb{Z}_8$ and

$$\mathcal{G} = \left\{(x, y) \in \mathbb{Z}^2 : 0 < y \leq 58, 0 \leq x < 862 - \frac{1}{4}y^2, \gcd(x, y) = 1\right\}.$$

If $(x, y) \in \mathcal{G}$ then by Corollary 1

$$\Omega(x^2 + 862y^2) \leq 8.$$

However, with the additional assumption that x is even we obtain by Corollary 2 much more:

$$\Omega(x^2 + 862y^2) \leq 5$$

Really, if $x = 2x_1$ then

$$x + y\sqrt{-862} = 2x_1 + y\sqrt{-862} \in \boldsymbol{p}$$

where $\boldsymbol{p}^2 = 2 \cdot \mathcal{O}_F$. By [6, Theorem 2] we have

$$D_{[\boldsymbol{p}]}(Cl(\mathcal{O}_F)) = 8 - \frac{8}{2} = 4$$

and hence our assertion. In particular for $y = 1$ we obtain

$$\Omega(x^2 + 862) \leq 8 \qquad \text{for } x = 0, 1, \ldots, 861$$

but

$$\Omega(2x^2 + 431) \leq 4 \qquad \text{for } x = 0, 1, \ldots, 430.$$

EXAMPLE 2. Let $F = \mathbb{Q}(\sqrt{-1555})$. Then $Cl(\mathcal{O}_F) \cong \mathbb{Z}_4$ and

$$\mathcal{G} = \left\{(x, y) \in \mathbb{Z}^2 : 0 < y \leq 39, -\frac{y}{2} \leq x < 389 - \frac{1}{4}(y + 1)^2, \gcd(x, y) = 1\right\}$$

Hence by Corollary 1

$$(x, y) \in \mathcal{G} \Longrightarrow \Omega(x^2 + xy + 389y^2) \leq 4.$$

Assuming additionally that $2x + y$ is divisible by 5 we find that $x^2 + xy + 389y^2$ is also divisible by 5 and hence similarly as above we obtain

$$\Omega\left(\frac{x^2 + xy + 389y^2)}{5}\right) \leq 2.$$

In particular for $y = 1$ we receive (after the substitution $x = 5k + 2$)

$$\Omega(5k^2 + 5k + 79) \leq 2 \qquad \text{for } k = 0, 1, \ldots, 77.$$

REFERENCES

1. W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.*, **139** (1994), 703–722.
2. H. B. Mann, Additive group theory—A progress report, *Bull. Am. Math. Soc.*, **79** (1973), 1069–1075.
3. M. Mazur, A note on the growth of Davenport's constant, *Manuscripta Math.*, **74** (1992), 229–235.
4. H. Möller, Verallgemeinerung eines Satzes von Rabinowitsch über imaginär-quadratische Zahlkörper, *J. Reine Ang. Math.*, **285** (1976), 100–113.
5. J. E. Olson, A combinatorial problem on finite Abelian groups, I, II, *J. Number Theory*, **1** (1969), 8–10, 195–199.
6. M. Skałba, On numbers with a unique representation by a binary quadratic form, *Acta Arithmetica*, **64** (1993), 59–68.
7. M. Skałba, The relative Davenport's constant of the group $\mathbb{Z}_n \times \mathbb{Z}_n$, *Grazer Math. Berichte*, **318** (1992), 167–168.

Received 27 March 1995 and accepted 22 July 1997

M. SKAŁBA
Institute of Mathematics,
Warsaw University,
Banacha 2,
02-097 Warsaw,
Poland